

Another problem is inadequate cooperation within the industry to manage the nationwide and international scope of organized call-sell operations. Cooperation is discouraged in several ways. First, the industry fears liability relating from sharing customer information. Second, right to privacy issues are a concern. Third, carriers are unwilling to share customer information because of the highly competitive nature of the marketplace.

The Commission should encourage and participate in the development and delivery of fraud-specific training programs for state and federal law enforcement agencies, prosecutors, and judges. The Commission should also work with Congress to ensure that a federal investigatory agency has the responsibility and resources for serious toll fraud investigation and prosecution.

Finally, the Commission should consider some form of exoneration from liability for companies who share customer-specific information during the course of and in support of the investigation and prosecution of organized subscription and toll fraud schemes. Such exoneration should extend to information shared between carriers and law enforcement agencies, even when legal process is not present, as well as claims from other carriers for toll charges incurred during the course of investigations into organized toll fraud operations. This latter requirement is important since there are cases in which a known fraudulently used line is kept in service to assist in a

toll fraud investigation. In those situations, a cooperative approach to liability is needed.

## VI. PART 68 CHANGES

We support the Commission's proposal to amend Part 68 of the Commission's Rules to require equipment manufacturers to provide warnings regarding the potential risk of toll fraud associated with use of the equipment.<sup>22</sup> However, warnings should not be the manufacturers' only requirement.

As suggested in the TFPC paper (Exhibit A), there are many minimum standards that manufacturers could be instructed to meet. At the very least, the Commission should require that the default codes in the PBX be set so that remote access is disabled. That way, businesses who want to have this function must make a conscious decision to have this function, and will be fully informed of the risks by the manufacturer when those parameters are changed. Also, the manufacturer should be required to list for the customer in writing the features and treatments that are necessary to protect against PBX compromise and abuse.

## VII. INCENTIVES

The Commission notes that many commentators stated that carriers have little incentive to invest in preventive

---

<sup>22</sup> NPRM, para. 40.

systems to minimize fraud.<sup>23</sup> The Commission must understand that monetary incentives are not the only incentives that work in the telecommunications market. For customers to be satisfied with their local phone company, customers need to be happy with their complete service. If the service is not secure and trustworthy, the LEC suffers. In an era where telecommunications services to business customers are getting more and more competitive, the trust of the customer is of paramount importance. As we have outlined above, we have taken many steps and been recognized in the industry for our leadership in toll fraud prevention and detection techniques. The Commission should not destroy the careful balance by imposing a shared liability system that bears no relationship to the risks and rewards of the particular service provider.

#### CONCLUSION

Toll fraud is pervasive and serious steps must be taken to prevent it, detect it and prosecute offenders. Prevention is the key. Customers must be educated as to the liability for and dangers of toll fraud. All players in the industry must meet minimum standards to prevent and deal with toll fraud. Liability for losses that do occur should

---

<sup>23</sup> NPRM, para. 41.

be based on control over the instrumentality and on business risks and rewards.

Respectfully submitted,

PACIFIC BELL  
NEVADA BELL

  
\_\_\_\_\_  
JAMES P. TUTHILL  
NANCY C. WOOLF

140 New Montgomery St., Rm. 1523  
San Francisco, California 94105  
(415) 542-7657

JAMES L. WURTZ

1275 Pennsylvania Avenue, N.W.  
Washington, D.C. 20004  
(202) 383-6472

Their Attorneys

Date: January 14, 1994



# **EXHIBIT A**

**A Cooperative Solution to the Fraud that Targets  
Telecom Systems**

**A Position Paper Developed by the  
Toll Fraud Prevention Committee  
of the  
Network Operations Forum**

## **TFPC POSITION PAPER ON PBX REMOTE ACCESS FRAUD**

The Toll Fraud Prevention Committee of the Alliance for Telecommunications Industry Solutions (formerly the Exchange Carrier Standards Association) has reviewed the problem of remote access fraud at private branch exchanges (PBXs), voice mail systems, and other customer premises equipment (CPE). Such fraud is a serious liability for business customers (and other customers) of telecommunications services, resulting in hundreds of millions of dollars of losses annually. To date, no one can say with any confidence that a solution has been found, or that the problem is under control.

Remote access fraud involves the penetration of a PBX or other CPE by one or more unauthorized callers, typically for the purpose of gaining access to restricted information or to network facilities where the defrauder cannot be charged for resulting calls. PBX remote access fraud is frequently used for "call sell" operations, where people pay defrauders to place unlimited calls to international destinations. Compromised access codes (800 or local numbers which reach Direct Inward System Access [DISA] ports and maintenance ports in the PBXs) have a commercial value of thousands of dollars in the toll fraud underworld. Criminals have a significant incentive, consequently, to penetrate telecommunications equipment for remote access fraud.

In analyzing this problem the TFPC determined that there are many actual or potential participants involved in providing CPE of every type to telecommunications users. It is reasonable to expect that each party will act responsibly when providing such equipment, to ensure that appropriate security against remote access fraud is included. The TFPC identified the following as industry segments that are involved in this issue:

- |  |                              |
|--|------------------------------|
| -- the business owner                              | -- local telephone companies |
| -- the consultant                                  | -- long distance carriers    |
| -- sales & installation firms                      | -- law enforcement agencies  |
| -- original equipment manufacturers                | -- legislators               |
| -- manufacturers of adjunct equipment              | -- insurers                  |
| -- marketers of secondary or refurbished equipment | -- consumer/user groups.     |

Many of these segments may be involved in an individual CPE configuration. The typical PBX goes through many steps: a needs assessment, equipment evaluation, purchase decision, equipment design, installation and testing, maintenance, ongoing use, and eventual retirement/replacement. Thus, it falls to many parties to evaluate the security of a telecommunications environment at progressive steps in the equipment's life cycle.

With this distribution of responsibility, security is often neglected. This simplifies enormously the task of defrauders, who persistently look for CPE with lax security to use for their illegal purposes. It is necessary to stress that the business owner, the owner or lessee of the CPE, has the primary and paramount care, custody, and control of the CPE.



## **TFPC POSITION PAPER PBX ACCESS FRAUD**

The owner has the responsibility to protect this asset, the telecommunications system, equally as well as other financial assets of the business. The PBX is vital to the business's health, since virtually every business survives and thrives by communicating with other businesses and customers. Abuse of the PBX by hackers, even to the disruption of its functioning, can carry a significant financial and operational penalty. Consequently, the business owner must assure that the PBX (and the entire telecommunications environment under the owner's control) is secure from penetration and abuse.

It is worth noting that this form of telecommunications fraud is a crime. Businesses, whether small firms or large corporations, are persons before the law. They also enjoy the same protections as other citizens, including protection from unlawful disruption of their operations and from theft. Therefore, defrauders of these corporate citizens should be prosecuted to the full extent of the law.

It is essential, therefore, that every industry segment support the integration of security into PBXs, voice mail systems, and other CPE. Some segments have a direct role, as is the case for the equipment manufacturer and the installation firm. Others, such as legislators and regulators, have a less direct, but still important role in the control of toll fraud in general, and remote access fraud in particular. The attachment to this position paper outlines the recommendations of the TFPC for each segment of the industry. For each there is a minimal requirement for preventive action, supported by additional steps that each party should take. These recommendations are not exhaustive of all preventive steps, nor will those that are adopted end remote access fraud. However, they will reduce the risks that industry currently faces.

In the judgment of the TFPC, coordination and cooperation are essential to achieving greater success in this area. Consequently, the TFPC urges each industry segment to deliver the maximum protection that it can identify, in supporting customers of telecommunications services.

Inquiries about this paper should be directed to the Toll Fraud Prevention Committee Secretary on 201-740-3573.

## **ATTACHMENT: SUGGESTED ANTI-FRAUD EFFORTS BY INDUSTRY SEGMENT**

### **RESPONSIBILITIES OF THE BUSINESS OWNER:**

The basic responsibility of the business owner is to devote adequate resources (time, talent, capital, etc.) to the selection of CPE and to its management, including fraud prevention, detection, and deterrence. It is an essential part of managing the business. The owner must demand that internal staff and supporting external professionals, such as consultants, include security concerns in the evaluation, design and operation of the telecommunication environment for his/her business.

Other efforts are highly recommended to assure that security matches the importance placed on efficiency, economy, accountability, etc., as considerations in PBX and CPE design.

- Enlist knowledgeable professional support (consultants, security experts) as needed.
- Include security as a prime consideration in the definition of system and user needs.
- Require suppliers to provide only the capabilities required/requested. Other features should be made known, with controls, restrictions, vulnerabilities clearly noted.
- Include security support in maintenance agreements. Identify emergency telephone numbers to be used on discovery or suspicion of fraudulent abuse.
- Define and implement an anti-fraud plan. Enlist employees in the plan; provide a feedback system for emergency alerts. Monitor and refine the plan.
- Manage the telecommunications system when installed: monitor usage continually; assign and encrypt passwords; restrict access in, out, and between interconnected nodes of the system; assure the compatibility and security of interconnected CPE.
- Enlist law enforcement agencies when victimized; preserve evidence for prosecution.
- Secure relevant documentation, to avoid compromise and piracy of data, passwords, etc.
- Secure access to the physical facilities, cabling, access ports, administrative terminals, etc.

### **RESPONSIBILITIES OF THE CONSULTANT:**

The consultant supports the business owner in deciding what type of equipment to buy, what type of services to install, and how to configure both equipment and services for the desired operational environment. It is the consultant's responsibility frequently to act in place of the owner. Consequently, the consultant has the same tasks as the owner. Trusted for special expertise, the consultant must place high among his/her priorities the establishment of a secure telecommunications environment. This requires that the consultant be very aware of any fraud implications regarding the system being recommended, and ensure that others involved (vendors, installation technicians, etc.) meet or exceed the levels of security needed. The consultant should take steps to ensure that security is cared at the time of installation and into the future.

Additional support efforts are appropriate:

- Understand all current fraud exposures with CPE, and know how to minimize, if not prevent, exposure in the current telecommunications environment.
- Consider security features when making a recommendation on equipment, and detail in writing to the owner the fraud exposure of the final configuration.
- Understand how features in the local and long distance carriers' services can be used to enhance the security of the equipment.
- Be knowledgeable of and make the owner aware of adjunct equipment that can help prevent and identify abuse.

#### **RESPONSIBILITIES OF THE SALES AND INSTALLATION FIRMS:**

The sales and installation firms, which will frequently provide ongoing service and maintenance of the CPE, should assist in educating the business owner about the risks and vulnerabilities of the equipment. While stressing the value of the system's features, the sales agents should make known the dangers of toll fraud.

Additional support efforts are appropriate:

- Be completely familiar with the system's features, including those subject to compromise and abuse, such as DISA, maintenance ports, least cost routing features, etc.
- Identify and change any default codes that control access to features and facilities that are subject to compromise and abuse. Secure such replacement codes with responsible management personnel.
- Deactivate features that are not needed, with the full knowledge of the customer.
- Establish time of day restrictions, such as no access to international calling at night and on weekends.
- Restrict access to facilities (WATS, public network "dial 9") and establish calling privileges/limits (internal, local, domestic, international) as appropriate.

#### **RESPONSIBILITIES OF THE MANUFACTURERS OF ORIGINAL AND ADJUNCT EQUIPMENT AND THE MARKETERS OF SECONDARY/ REFURBISHED EQUIPMENT:**

These industry segments play a special role in protecting the industry from toll fraud. These manufacturers must develop and deploy flexible and effective security protections to complement the advanced telecommunications features required by businesses. In many cases customers are not aware of the need for such protections and do not request them. They are often unaware of the vulnerabilities of an unprotected system and of the dogged drive of the hacker to find new PBXs to abuse.

Additional support efforts are appropriate:

- List in writing for the customer the features and treatments that are necessary to protect against PBX compromise and abuse.
- Ship only those features that the customer requests; remove default passwords from features such as DISA, so that hackers cannot easily access them.
- Secure in writing that the customer is aware of the system's capabilities and protections.
- Provide emergency contact numbers for customers to use in cases of compromise and abuse.
- Make upgrades to the CPE's controlling software by methods more secure than a dial-up modem with default passwords. For example, update the customer's CPE through call back modems or secure token access devices.
- Care for the security and compatibility of adjunct and refurbished equipment with other interconnected segments of the customer's network.
- Educate the customer thoroughly, including support for user groups, etc.

#### **RESPONSIBILITIES OF THE LOCAL TELEPHONE COMPANIES:**

The local telephone companies (LECs) have a supporting role for customers who choose their own PBX and CPE. The LECs may frequently not know what a customer is planning. Nor are the LECs familiar with the wide variety of terminal equipment that is available to business owners. However, they can help to combat fraud by promoting an heightened security concern among all their customers.

Other suggested efforts include:

- Conduct wide customer education through bill inserts, addressing end user groups, holding training seminars, etc.
- Evaluate permitted teaming efforts with long distance companies, equipment manufacturers, etc. to educate customers.
- Evaluate all LEC products and services for security concerns before deployment.
- Where tariffed telecommunications systems are offered, fulfill the above suggested security functions of manufacturer and consultant, as appropriate.
- Alert their customer contact personnel (business office, repair, sales/service) to the signs of toll fraud, so that these staffs can better support business owners who are victimized.
- \* --Deploy network blocking services (such as International Direct Dial Blocking) and call screening information digits to complement customer equipment restriction strategies and long distance company network monitoring.
- Develop network monitoring capabilities to highlight potential fraud patterns (local hacking, 800, international, etc.) as early as possible.
- Expand centralized fraud bureau support to a seven day/24 hour basis.
- Continue the use of security staffs to support long distance company investigations and customer inquiries.
- Cooperate with law enforcement agencies in education, investigation, and prosecution efforts.
- Develop case documentation for federal and local regulators, in support of guidelines allowing timely and responsive security efforts in cases of toll fraud.

## **RESPONSIBILITIES OF THE LONG DISTANCE COMPANIES:**

The long distance companies (IXCs) are frequently the networks that bear the brunt of toll fraud, because fraudulent calls are often directed to international destinations. IXCs assist in protecting their customers with a variety of monitoring capabilities and protection (indemnity) plans. IXCs also can combat fraud by continuing the extensive educational campaigns to all customers.

Other suggested efforts include:

- Perform network monitoring of 800 calling and calls directed to international destinations, to identify suspected fraud patterns.
- Alert their customer contact personnel (business office, operator services, repair, sales/service) to the signs of toll fraud, so that these staffs can better support business owners who are victimized.
- Include in their network sales efforts educational security information that will alert customers to network vulnerabilities and suggest effective protections.
- Continue the use of security staffs to support customer inquiries.
- Cooperate with law enforcement agencies in education, investigation, and prosecution efforts.
- Develop case documentation for federal and local regulators, in support of guidelines allowing timely and responsive security efforts in cases of toll fraud.

## **RESPONSIBILITIES OF REGULATORS:**

Regulators perform a critical task in defining how the market acts and reacts. In the case of toll fraud, regulators should recognize that it costs the telecommunications industry (and ultimately consumers and shareholders) billions of dollars annually. Those best able to combat fraud should be empowered to take timely and effective steps to minimize its incidence and severity. In some cases regulatory guidelines might appear to prevent LECs and/or IXCs from disconnecting defrauders in a timely manner. Companies that operate across many states are frequently subject to conflicting rules that do not reflect the realities of systematic, professional toll fraud. Confusion over rules covering collection and security activities allows defrauders to stay on the network. Regulators should act to clarify such areas.

Additional suggestions are:

- Cooperate across jurisdictions (e.g., through NARUC, the FCC) to standardize regulations that allow timely and effective responses against toll fraud.
- Alert customers through periodic press releases about the vulnerabilities of toll fraud and their responsibilities to take effective precautions.
- Stimulate effective legislation punishing toll fraud, and promote its enforcement.
- Allow LECs to deny service, both before it is established and after installation takes place, when warranted by suspected fraud.
- Allow telecommunications service providers to cooperate in combating toll fraud through the exchange of customer information.

## **RESPONSIBILITIES OF LEGISLATORS:**

Legislators help create the telecommunications environment in response to the drive of technology and market forces. It is essential that they foster a legislative environment in which telecommunications service providers can bring their full skills to the prevention, detection, and deterrence of toll fraud, recognizing that toll fraud is a professional endeavor that continually adapts.

Other steps are:

- Create no anti-fraud mandates that pit segments of the industry against each other, or that allow one segment to avoid responsibility for contributing to the solution.
- Create incentives for the industry to work cooperatively against the problem.
- Support and finance the efforts of law enforcement organizations, so that they are empowered to pursue and prosecute perpetrators of toll fraud.
- Amend the penal codes to remove the relative impunity enjoyed by those who engage in toll fraud as a profession.

## **RESPONSIBILITIES OF INSURERS:**

Insurers can expand the attention that toll fraud receives by including coverage for toll fraud liability in their product portfolios. Insurers can contribute greatly to the education of business customers by discussing risks and protections related to toll fraud, together or separately with other risk coverage that virtually all businesses consider. Packaging and pricing toll fraud liability coverage affordably (yet profitably) will prompt businesses to take effective precautions. This, in turn, will reduce the incidence of remote access fraud.

## **RESPONSIBILITIES OF END USER GROUPS:**

Trade associations and telecommunications end user groups can also broadcast that toll fraud is a significant risk for businesses. Education from many sides will reinforce the necessity for protective action. User groups are particularly valuable in this mode. Frequently, they are aligned by their use of a single technology or a single vendor. Consequently, they can readily share both negative experiences and effective remedies. These groups can also provide the "critical mass" needed to stimulate development of new technology.

## **RESPONSIBILITIES OF LAW ENFORCEMENT AGENCIES:**

While toll fraud might appear as a victimless crime, or one of less pressing priority for prosecution, nevertheless, the operational and financial harm done to businesses by telecommunications defrauders is substantial. Federal and state laws variously define telecommunications fraud and place enforcement responsibilities in many organizations. It is important that this distribution not hinder timely investigations and effective enforcement. Police officers should cooperate across jurisdictions to investigate suspected cases, and district attorneys should prosecute cases to deter future toll fraud and gain restitution for victimized businesses. The enforcement community can also aid the essential educational effort through its own support of end user groups, business councils, etc.

**Subscription Fraud**  
**(External)**

It's a billion-dollar-a year business that's getting bigger every year. The United States Secret Service estimates that telecommunications fraud exceeded \$1.2 billion in 1991.

Consumers in every state are paying more than they need to because of fraud and the issue is of legitimate concern to regulators, local and long distance companies alike.

Only through the concerted efforts of everyone affected by fraud will its costly impact be reduced, if not eliminated.

There are many types of telecommunications fraud; one of the most pernicious is Subscription Fraud.

A legitimate question to ask is: If the industry is aware of the problem, why doesn't it establish procedures to eliminate the fraud? And the answer is: Many procedures are in place to identify and prevent potential fraud, but more weapons are needed to successfully combat those who conspire to defraud local and long distance companies.

In some cases, regulatory guidelines designed to promote universal service frequently enable the person intent on fraud to gain access to the network with a minimum of verifiable references. Long distance companies, which frequently suffer the largest loss from fraud, do not have any input prior to a subscriber signing up for their service. Rather, they are notified of their selection after the fact. The fraud, however, begins immediately.

Calls are made to and bridged between countries that have no direct communication links, such as the Middle East. Calls from restricted telephones such as prison telephones or coin telephones are accepted "collect" and then relayed to distant points.

In transportation centers or on street corners, fraudulent "call sell" operations are established. A local telephone operator, when checking for authorization to bill a call to the account, will receive positive, but fraudulent, acceptance. Losses of \$20,000 to \$30,000 in a single day have been generated.

What can be done to correct this vulnerability, to protect the consumers who ultimately pick up the tab? There are no easy answers, but each party can play a significant role: the local telephone company, the long distance company, state and federal regulators, legislators and consumers.

**The local telephone company** is the first point of contact, where the network connection is made. While it might seem easy to keep fraudulent customers off the network, it is difficult in practice. Local telephone companies can improve their effectiveness by following these steps:

- **Initial Service Request** - Local telephone company representatives should be aware of the typical profile of an account set up for subscription fraud.

- **Installation Service** - Installation technicians can provide excellent intelligence before fraud starts. Virtually every location requires on-site work, since multiple lines are ordered. The installer also will be one who can identify anyone on the premise should an arrest occur.
- **Customer Service** - Telephone accounting systems frequently use billing thresholds called high toll notifiers. The local telephone company should evaluate the feasibility of developing programs to improve early detection. Further investigation would be necessary to demonstrate whether or not fraud has been committed. Moreover, where special billing and collection contracts exist between local telephone and long distance companies, additional steps can be developed.
- **Security Department**- The privacy of communications is a guiding principle for local telephone companies and there are well defined procedures and regulations on what can be done in pursuing leads or divulging findings to external parties. The operations of the local telephone company's Security Department properly allow for the detection of billing evasion schemes, including accumulation of data that can be used in a court of law. Consequently, security managers should work closely with their internal coordinates to investigate suspect accounts.
- **Product Development** - Data base services which support alternate billing services can be enhanced to offer added protection. Thresholds to count collect and bill to third number attempts can be deployed. New products and services should be analyzed for fraud implications prior to deployment. Enhancements to billing systems should facilitate the identification and tracking of fraud losses.

Long distance companies have an incentive to identify subscription fraud. A long distance company that protects its own network (e.g., by blocking calls from a problem telephone line) can help protect the industry as well. The long distance company can work cooperatively with the local telephone company through their respective security departments. In that way, efforts to investigate accounts, document any abuse, and shut down the fraud) including involvement of the appropriate law enforcement agencies) will help prevent its migrating to another company.

Where a contract for billing exists between the long distance and local telephone companies, the long distance company should arrange to accelerate delivery of billing tapes. Delivery at long intervals (e.g., every 30 days) virtually eliminates the value of the local telephone company's high toll notifier systems. Rather, such delays make it likely that a long distance company will be victimized by defrauders.

Regulators need to recognize and support the industry's growing need to reduce telecommunications fraud. Losses are not always easily quantified and may not appear to impact state residents (e.g., international calls are under interstate jurisdiction). Nevertheless, losses are enormous in the aggregate, and significant harm is done in the local market. The long distance companies recover these losses from legitimate callers. The local telephone company must also recover its administrative expenses (negotiation, installation, investigation, disconnection, adjustments, etc.), as well as losses from line rentals and local usage.



Regulators' concerns about nondiscrimination and privacy are shared by all. However, regulators need to permit the local telephone company sufficient flexibility--when negotiating new service--to take legitimate precautions to protect itself, its rate payers, and indeed, even the industry. This may include requiring positive identification from applications. Some greater latitude is also appropriate when the telephone company suspects that fraud will likely generate large uncollectibles, as with Subscription Fraud. Timely pre-billing corrective action should take place so that losses do not escalate, while, for example, written warnings of suspension are mailed.

Telephone customers can play an important role by reporting incidents of suspected fraud to their local telephone company business offices. Caution is appropriate, and their timely referrals are appreciated.

Subscription Fraud--and all telecommunications fraud--penalizes each consumer, the industry, and the whole economy. No one segment of the industry can combat fraud effectively, but concerted action can change the trend line of mushrooming losses. Above all, flexibility and speedy cooperation are needed. One must remember that fraud is big business, and the returns are dramatic. One can expect that the defrauders will be as imaginative and resilient in the future as they have been in the past. So must be those who will battle telecommunications fraud.

**EXHIBIT B**



# **EXHIBIT B**

# PACIFIC BELL LOCKON<sup>SM</sup>



Telephone

Toll Fraud

Protection



PACIFIC  BELL

A substantial portion of the materials contained herein are copyrighted® by Telecommunications Advisors, Inc. (1992) and are reproduced herein by Pacific Bell pursuant to a licensing agreement with Telecommunications Advisors, Inc. No part of this book may be reproduced in any way, stored in a retrieval system, or transmitted in any form or by any means, whether electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of Telecommunications Advisors, Inc. of Portland, Oregon.



## FOREWORD

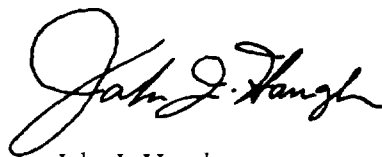
Toll fraud has become the modern day scourge of telecommunications systems. "Hackers" and their allies penetrate systems probing for weaknesses. Once they learn how to compromise systems, the information is transferred and sold to criminals, who resell stolen long-distance access at the "retail" (street) level. Unsuspecting businesses are then charged for long-distance calls made to locations around the world.

Pacific Bell is the first local telecommunications company in the country to have prepared an extensive handbook to help consultants and users protect systems from penetration and loss. We are pleased to have been associated with the company in the process of making this handbook available and commend Pacific Bell for its efforts.

Users must become more security conscious. Hardware and software applications have made modern telecommunications systems a "wonder to behold"—with numerous feature-rich applications that allow economical and virtually instantaneous communications. These same systems, however, are also vulnerable. Pacific Bell's handbook will be of significant assistance in walking users and consultants through the steps necessary to protect telecommunications systems and equipment.

Pacific Bell has adopted a positive, proactive approach in working with the consultant and user community to combat fraud and theft. We congratulate the company's management and staff for having taken this pacesetting approach.

Sincerely,

A handwritten signature in black ink, reading "John J. Haugh". The signature is fluid and cursive, with the first letters of each word being capitalized and prominent.

John J. Haugh  
Chairman  
Telecommunications Advisors, Inc.

John J. Haugh is Chairman of Telecommunications Advisors, Inc. (TAI), a consulting firm located in Portland, Oregon. As a nationally recognized expert on telecommunications and network security issues, Mr. Haugh writes and lectures regularly on these subjects. He is principal author of a two-volume reference work, Toll Fraud and Telabuse, published by TAI in 1992, as well as editor of the journal, Telecom & Network Security Review, published six times yearly by TAI.

## CONTENTS

Introduction .....	4
Chapter 1 Toll Fraud: an Overview .....	5
Toll Fraud Defined .....	5
Annual Cost of CPE Toll Fraud .....	6
Liability for Toll Fraud .....	7
CPE Owner Liability .....	8
Evolution of Toll Fraud .....	8
First Amendment Issues .....	10
The Drug Culture and Organized Crime Connection .....	10
Hardware and Software for Hackers .....	11
Tapping a Lucrative Market: Recent Immigrants .....	12
The “Retailers” of Stolen Long-Distance Service .....	12
Toll Fraud Centers: Where the Calls Go .....	13
Chapter 2 PBX Toll Fraud .....	15
Evaluate the Need for Remote Access .....	15
Other Types of Remote Access Fraud .....	21
Toll Fraud Indicators .....	23
Operational PBX Toll Fraud Indicators .....	23
Statistical Indicators of Potential CPE Toll Fraud .....	24
Chapter 3 Voice Mail Toll Fraud .....	27
Voice Mail System Toll Fraud Indicators	
Operational VMS Toll Fraud Indicators .....	33
Statistical Indicators of Potential CPE Toll Fraud .....	33
Chapter 4 Call Diverter Toll Fraud .....	35
Operational Call Diverter Toll Fraud Indicators .....	36
Chapter 5 Auto Attendant Toll Fraud .....	37
Chapter 6 CPE Port Toll Fraud ... ..	39
CPE Port Toll Fraud Indicators .....	42



Chapter 7	Pager Toll Fraud .....	43
Chapter 8	Prosecuting the Culprits .....	45
Chapter 9	Pacific Bell LockOn is Your Assurance of Protection Against Telephone Toll Fraud .....	47
	Prevention .....	47
	Detection and Intervention .....	47
	Prosecution .....	48
Chapter 10	Centrex—Toll Fraud Prevention .....	49
Chapter 11	Toll Fraud Prevention Checklists .....	51
	PBX Toll Fraud Prevention Checklist .....	52
	Voice Mail Toll Fraud Checklist .....	56
	Call Diverter Toll Fraud Checklist .....	59
	Auto Attendant Toll Fraud Checklist .....	60
	CPE Port Toll Fraud Checklist .....	62